

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22

	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	2037	2038	2039	2040	2041	2042	2043	2044	2045	2046	2047	2048	2049	2050	2051	2052	2053	2054	2055	2056	2057	2058	2059	2060	2061	2062	2063	2064	2065	2066	2067	2068	2069	2070	2071	2072	2073	2074	2075	2076	2077	2078	2079	2080	2081	2082	2083	2084	2085	2086	2087	2088	2089	2090	2091	2092	2093	2094	2095	2096	2097	2098	2099	2100	2101	2102	2103	2104	2105	2106	2107	2108	2109	2110	2111	2112	2113	2114	2115	2116	2117	2118	2119	2120	2121	2122	2123	2124	2125	2126	2127	2128	2129	2130	2131	2132	2133	2134	2135	2136	2137	2138	2139	2140	2141	2142	2143	2144	2145	2146	2147	2148	2149	2150	2151	2152	2153	2154	2155	2156	2157	2158	2159	2160	2161	2162	2163	2164	2165	2166	2167	2168	2169	2170	2171	2172	2173	2174	2175	2176	2177	2178	2179	2180	2181	2182	2183	2184	2185	2186	2187	2188	2189	2190	2191	2192	2193	2194	2195	2196	2197	2198	2199	2200	2201	2202	2203	2204	2205	2206	2207	2208	2209	2210	2211	2212	2213	2214	2215	2216	2217	2218	2219	2220	2221	2222	2223	2224	2225	2226	2227	2228	2229	2230	2231	2232	2233	2234	2235	2236	2237	2238	2239	2240	2241	2242	2243	2244	2245	2246	2247	2248	2249	2250	2251	2252	2253	2254	2255	2256	2257	2258	2259	2260	2261	2262	2263	2264	2265	2266	2267	2268	2269	2270	2271	2272	2273	2274	2275	2276	2277	2278	2279	2280	2281	2282	2283	2284	2285	2286	2287	2288	2289	2290	2291	2292	2293	2294	2295	2296	2297	2298	2299	2300	2301	2302	2303	2304	2305	2306	2307	2308	2309	2310	2311	2312	2313	2314	2315	2316	2317	2318	2319	2320	2321	2322	2323	2324	2325	2326	2327	2328	2329	2330	2331	2332	2333	2334	2335	2336	2337	2338	2339	2340	2341	2342	2343	2344	2345	2346	2347	2348	2349	2350	2351	2352	2353	2354	2355	2356	2357	2358	2359	2360	2361	2362	2363	2364	2365	2366	2367	2368	2369	2370	2371	2372	2373	2374	2375	2376	2377	2378	2379	2380	2381	2382	2383	2384	2385	2386	2387	2388	2389	2390	2391	2392	2393	2394	2395	2396	2397	2398	2399	2400	2401	2402	2403	2404	2405	2406	2407	2408	2409	2410	2411	2412	2413	2414	2415	2416	2417	2418	2419	2420	2421	2422	2423	2424	2425	2426	2427	2428	2429	2430	2431	2432	2
--	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	---

The present invention relates to the field of computer network management. It specifically concerns secure data exchange over a computer network. More particularly, the present invention relates to securely proving ownership of pseudonymous or anonymous electronic receipts.

10
11
12
13
14
15
16
17

18
19
20
21
22

Since the mid 1990s one of the most rapidly growing retail sectors is referred to as electronic commerce. Electronic commerce involves the use of the Internet and proprietary networks to facilitate business-to-business, consumer, and auction sales of everything imaginable, from computers and electronics to books, recordings, automobiles, and real estate. In such an environment consumer privacy is becoming a major concern.

However, the mere fact that electronic commerce is conducted over an existing open network infrastructure such as the Internet runs counter to the privacy of the consumer. Often, there are legitimate reasons for a party to remain anonymous.

A method is known from US 6,061,789, for an anonymous, provable information exchange between a sender and an addressee in a computer network. The computer network providing a public key infrastructure, advantageously with certification, and an anonymous communication channel available between network users. The sender composes an offer request with a subject or merchandise description and a digital signature of the sender. The request is transmitted via the anonymous communication channel to at least one addressee. The addressee composes a reply with an offer description and its digital signature, the digital signature being computed over a selection of quantities comprising at least one of merchandise description, offer description, signature of sender, and further including the addressee's public key or public key certificate. Upon receiving the reply the sender uses the merchant's public key, known, transmitted, or extracted from the public key certificate, to encrypt the received digital signature of the merchant, thus determining a first temporary value, the sender computes a concatenation of the selection of quantities on which the merchant's signature is based, thus determining a second temporary value. The sender compares the temporary values, whereby a match indicates genuineness of the offer. Moreover, the merchant is able to make sure that the offer and the merchandise are given to the same consumer, i.e., the customer cannot freely transfer the offer to another consumer. This entails the consumer to reveal his or her identity to the merchant, but only when the consumer is ready to purchase the merchandise, but not before.

1 Summary of the Invention

2 It is therefore an aspect of the present invention to
3 provide methods, apparatus and systems for securely proving
4 ownership of pseudonymous or anonymous electronic receipts,
5 wherein a party that proves its ownership of the receipt can
6 stay anonymous, i.e., it does not need to reveal its
7 identity.

8 The foregoing aspect is achieved by a method, apparatus and
9 system as described and claimed. Further aspects and
10 advantageous embodiments of the present invention are
11 described and taught in the following description. The
12 aspects, features and advantages of the present invention,
13 will be apparent in the following detailed written
14 description.

15 Since more than one party is generally involved in the
16 communication and the exchange of data in accordance with
17 the present invention, parts of the description and some of
18 the claims take the perspective of each of the different
19 participants.

20 Brief Description of the Drawings

21 The novel features of the invention are set forth in the
22 description and the appended claims. The invention itself,
23 however, as well as a advantageous mode of use, further
24 aspects, and advantages thereof, will best be understood by
25 reference to the following detailed description of an

1 illustrative embodiment when read in conjunction with the
2 accompanying drawings, wherein:

3 Fig. 1 shows a general layout of a communication environment
4 in which the invention can be used;

5 Fig. 2 shows a data exchange according to a first embodiment
6 of the present invention;

7 Fig. 3 shows a data exchange according to a second
8 embodiment of the present invention;

9 Fig. 4 shows a data exchange according to a third embodiment
10 of the present invention;

11 Fig. 5 shows a data exchange according to a fourth
12 embodiment of the present invention; and

13 Fig. 6 shows a data exchange according to a fifth embodiment
14 of the present invention.

15 Detailed Description of the Invention

16 As the collection and exploitation of private information
17 become more of a concern, users are less willing to give out
18 information, and may want to conduct transactions under a
19 pseudonym or anonymously. For example, a user in a
20 pseudonymous or anonymous transaction may receive a receipt
21 of the transaction, e.g., a receipt of a payment. The user
22 might want to use the receipt at a later point in time or

1 several times in the future to prove that the particular
2 transaction took place, e.g., that the user made a payment.

3 The methods apparatus and systems for proving ownership of
4 an electronic receipt in accordance with the present
5 invention is to be used in a communication system providing
6 a public key encryption infrastructure. That is a system of
7 public key encryption using digital certificates from
8 certificate authorities and other registration authorities
9 that verify and authenticate the validity of each party
10 involved in an electronic transaction. The certificate
11 authority, also called "Trusted Third Party", is an entity,
12 typically a company, that issues digital certificates to
13 other entities like organizations or individuals to allow
14 them to prove their identity to others. The certificate
15 authority might be an external company that offers digital
16 certificate services or it might be an internal organization
17 such as a corporate MIS (Management Information System)
18 department. The Certificate Authority's chief function is
19 to verify the identity of entities and issue digital
20 certificates attesting to that identity.

21 In comparison, public key encryption is an encryption
22 scheme, where each person gets a pair of keys, called the
23 public key and the private key. Each person's public key is
24 published while the private key is kept secret. Messages
25 are encrypted using the intended recipient's public key and
26 can only be decrypted using his private key. This is
27 mechanism can also be used for or in conjunction with a
28 digital signature.

FOIA b 7 - D

1 The digital signature is formed by extra data appended to a
2 message which identifies and authenticates the sender and
3 message data using public-key encryption. The sender uses a
4 one-way hash function to generate a hash-code of, for
5 example, 32 bits from the message data. He then encrypts
6 the hash-code with his private key. The receiver computes
7 the hash-code from the data as well and decrypts the
8 received hash with the sender's public key. If the two
9 hash-codes are equal, the receiver can be sure that data has
10 not been corrupted and that it came from the given sender.

11 The need for sender and receiver to share secret
12 information, e.g., keys, via some secure channel is
13 eliminated, since all communications involve only public
14 keys, and no private key is ever transmitted or shared.
15 Public-key encryption can be used for authentication,
16 confidentiality, integrity and non-repudiation. RSA
17 encryption is an example of a public-key cryptography
18 system.

19 The one-way hash function, also called "message digest
20 function", used for the digital signature is a function
21 which takes a variable-length message and produces a
22 fixed-length hash. Given the hash it is computationally
23 impossible to find a message with that hash. In fact, one
24 cannot determine any usable information about a message with
25 that hash, not even a single bit. For some one-way hash
26 functions it is also computationally impossible to determine
27 two messages which produce the same hash. A one-way hash
28 function can be private or public, just like an encryption
29 function. A public one-way hash function can be used to
30 speed up a public-key digital signature system. Rather than

1 signing a long message which can take a long time, the
2 one-way hash of the message is computed, and the hash is
3 digitally signed.

4 The method and system according to the present invention
5 works as follows: A sender creates a first message to be
6 sent to a first addressee including a transaction request
7 and a reference to a designated owner of a receipt to be
8 generated in response of receiving the message. The sender
9 signs the message using a first secret signature key and
10 sends it to the first addressee.

11 The first addressee receives the message from the sender and
12 authenticates it using a public signature verification key
13 associated to the secret signature key held by the sender of
14 the message. Then the first addressee issues a receipt
15 including the reference to the designated owner of the
16 receipt and details for what the receipt has been given and
17 signs the receipt with a public signature key assigned to
18 the first addressee issuing the receipt. Finally, the first
19 addressee returns the receipt to the sender of the message.

20 In response, the sender receives the receipt from the first
21 addressee. In case the sender is different from the
22 designated owner of the receipt, the receipt is transferred
23 from the sender to the designated owner. However, in order
24 to prove ownership the sender, in case he is the designated
25 owner, or the designated owner himself composes a second
26 message including the receipt, signs it using a second
27 secret signature key and sends it to a second addressee.

1 The second addressee, in return, receives the second message
 2 from the sender, obtains a public signature verification key
 3 on the basis of the reference to the owner of the receipt
 4 and examines whether or not the secret signature key used
 5 for signing the second message is associated to the public
 6 signature verification key obtained on the basis of the
 7 reference to the owner of the receipt. In case of match the
 8 second addressee can be sure that he received the receipt
 9 from the owner of the receipt. However, the first and
 10 second addressee can also be the same party.

11 A major advantage of the method and system in accordance
 12 with the present invention is that in a pseudonymous or
 13 anonymous transaction based system it is now possible to
 14 remain anonymous or pseudonymous when presenting electronic
 15 receipts, while securely proving ownership of the receipt.
 16 Another advantage is that the inventive method and system
 17 can as well be implemented in existing communication
 18 networks providing a public key encryption infrastructure,
 19 such as the Internet.

20 With reference to Fig. 1, the general layout of a
 21 communication environment is described in which the
 22 invention can be used. A user 100 is able to communicate
 23 with a transaction server 102 over a communication
 24 connection 104. It is assumed that the user possesses
 25 long-term credentials, such as a secret key SKu, a public
 26 key PKu and a public key certificate CERTu that allows the
 27 user 100 to prove his identity to others. The long term
 28 credentials are linked to the user 100 over a long time,
 29 e.g., lifetime. Generally, they can be used for

1 transactions as well, though, not providing anonymity or
2 allowing pseudonymous transactions.

3 Now, in a pseudonymous or anonymous setting in accordance
4 with the present invention, a Pseudonym Certificate Issuer
5 (PCI) 106 is established for granting short-lived
6 pseudonymous certificates for users. In the present case,
7 the user 100 requests a short-lived pseudonymous certificate
8 for a pseudonym P over a communication connection 108
9 linking the user 100 to the PCI 106. In return, the PCI 106
10 grants a short-lived pseudonymous certificate CERTp for the
11 user's 100 pseudonym P.

12 The needs for such a system in which the subject matter of
13 the present invention might be used is most advantageous
14 such when the system is secure, i.e., only the legitimate
15 user 100 can get a pseudonym certificate and the linking
16 between P and U can be revealed if necessary, e.g., in case
17 of fraud, and the PCI 106 cannot falsely incriminate the
18 user 100. Furthermore, user 100 can use receipts for
19 transactions without revealing his identity. Although the
20 system security, is important for the functioning of the
21 overall system, it has to be acknowledged that there are
22 known ways to ensure it. However, for the embodiments
23 described it is assumed that such a secure system is
24 implemented. Thus, the main focus is on the second issue,
25 how to prove ownership of an electronic receipt without
26 revealing identity.

27 Having the pseudonym P and the respective certificate CERTp
28 the user 100 can now perform transactions with the
29 transaction server 102 using the pseudonym P. A transaction

1 request under the pseudonym P is signed with a respective
2 secret key SKp. SKp may be known by either the PCI 106 or
3 the user 100, depending on the role the PCI 106 plays in the
4 pseudonymous system. The PCI 106 can, for example, act as
5 the user's proxy by generating PKp and SKp and acting as the
6 user 100. Alternatively, the user 100 generates the keys
7 PKp and SKp and the PCI 106 issues the respective
8 certificate CERTp for PKp.

9 For a pseudonymous transaction the user 100 sends the
10 transaction request to the transaction server 102. The
11 transactions requested can be any kind of business commonly
12 referred to as electronic commerce.

13 Whereby, electronic commerce summarizes conducting of
14 business communication and transactions over networks and
15 through computers. As most restrictively defined,
16 electronic commerce is the buying and selling of goods and
17 services, and the transfer of funds, through digital
18 communications. However electronic commerce also includes
19 all intercompany and intra-company functions, such as
20 marketing, finance, manufacturing, selling, and negotiation,
21 that enable commerce and use electronic mail, file transfer,
22 fax, video conferencing, workflow, or interaction with a
23 remote computer. Electronic commerce also includes buying
24 and selling over the World Wide Web and the Internet,
25 electronic funds transfer, smart cards, digital cash, and
26 all other ways of doing business over digital networks.

27 After the transaction server 102 concluded the transaction,
28 a receipt is issued and returned to the user 100. Later
29 when the user wants to prove to be the legitimate owner of

1 the receipt, he sends a validation request and the receipt
2 to a validation server 110 over a communication connection
3 112. It is understood that the transaction server 102 and
4 the validation server 110 can belong to the same business
5 entity or can even be implemented on the same computer
6 system.

7 The transaction server 102 and the validation server 110 are
8 also connected to the PCI 106 over communication connections
9 116 and 114. Over these connections the servers can obtain
10 the respective certificate CERTp issued for the pseudonym P
11 used by the user 100. Alternatively, the certificate CERTp
12 can also be transmitted together with the transaction
13 request and the validation request respectively.

14 Now with reference to Fig. 2, there is depicted the data
15 exchange according to a first embodiment of the present
16 invention. Block 200 illustrates a user and block 202
17 illustrates a Pseudonym Certificate Issuer (PCI)
18 communicating with each other. First, the user requests a
19 certificate from the PCI that is to be issued for a
20 pseudonym P the user intends to use for future transactions.
21 In the present case the user provides the pseudonym P to the
22 PCI. However, it might be desirable to have the PCI not
23 only issuing the certificates but also the pseudonyms. This
24 can be advantageous if many users ask for the same
25 pseudonym.

26 Furthermore, the user sends two public keys PK1_P and PK2_P
27 to be linked to the pseudonym P. The two public keys PK1_P
28 and PK2_P are associated to two private keys SK1_P and SK2_P
29 the user keeps as a secret. The private keys are used to

1 sign messages under the pseudonym P for initiating a
2 transaction and for proving the ownership of a receipt to be
3 issued in response to the transaction respectively.

4 In the present case it is advantageous to be able to link
5 the pseudonym P to the user, e.g., to be able to track down
6 fraudulent users. Therefore, the user is asked to transmit
7 a certificate CERTu to the PCI which allows to verify the
8 identity of the user. Hence, the message the user sends to
9 the PCI includes the pseudonym P and the user's personal
10 certificate CERTu and the two public keys PK1_P and PK2_P.
11 In order to ensure that the message has not been altered or
12 counterfeit, it is signed by the user using a personal
13 secret key SK_U as indicated by SIG_U.

14 In response to the certificate request the PCI returns two
15 certificates to the user. The certificates securely links
16 the public keys PK1_P and PK2_P to the pseudonym P. The
17 certificate further comprises the name of the issuer, here
18 PCI, and validity information, e.g. an expiry date of the
19 certificate. The contents of the certificate are of course
20 signed by the PCI in order to ensure that the certificate
21 has not been altered or counterfeit.

22 Focusing now on block 204, block 204 illustrates the user
23 previously exchanging data with the PCI and block 206
24 illustrates a transaction server TS communicating with each
25 other. The user intends to initiate a transaction.
26 Therefore, the user creates a transaction request message.
27 The transaction request message includes the transaction
28 relevant data TRX_P, such as an order or purchase
29 description, a specification of a payment method, an amount

1 of money to be paid, a specification of the currency.
2 Furthermore, the message includes the name of the addressee,
3 here the transaction server TS, and the pseudonym P used by
4 the user. Finally, the message is signed by the user using
5 the private key SK1_P as indicated by SIG1_P.

6 In return, the transaction server performs the requested
7 transaction, for example, accepts a payment. After
8 concluding the transaction the transaction server TS issues
9 a receipt acknowledging that the requested transaction has
10 been performed. The receipt is a message signed by the
11 issuer, here the transaction server TS as indicated by
12 SIG_TS. The message includes transaction relevant data
13 TRX_T composed by the transaction server TS, the pseudonym P
14 used by the initiator of the request taken from the
15 transaction request message and the issuer of the receipt,
16 here the transaction server TS.

17 Next, the user wants to prove that he is the legitimate
18 owner of the receipt received from the transaction server.
19 Block 208 illustrates the user previously received the
20 receipt and block 210 illustrates a validation server VS1
21 communicating to each other. First of all, the user sends
22 the previously received receipt to the validation server
23 VS1. Additionally, the user sends a message proving that he
24 is acting legitimately using the pseudonym P. In fact, the
25 user sends a message comprising the pseudonym P and two
26 randomizer R1 and R2 that is signed with the private key
27 SK2_P as indicated by SIG2_P.

28 In response, the validation server obtains the public key
29 PK2_P either from the PCI or from a respective certificate

1 securely linking the pseudonym P to the public key PK2_P
2 (not shown). Using the public key PK2_P the validation
3 server is able to authenticate whether or not the message
4 has been signed by the user legitimately using the pseudonym
5 P. This resulting from the fact that only the legitimate
6 user knows the private key SK2_P that was used to sign the
7 message. In order to ensure that the receipt itself has not
8 been altered or counterfeited the transaction server
9 authenticates the receipt as well using a certificate issued
10 for the transaction server TS by a certificate authority or
11 by obtaining the respective key directly from the
12 transaction server TS.

13 Alternatively, the user only sends one message as depicted
14 in the data exchange between block 212 illustrating the user
15 owning the receipt and an alternative validation server VS2.
16 In this case, the user composes a message consisting of the
17 receipt previously received from the transaction server and
18 two randomizer R1 and R2. The validation server again
19 obtains the public key PK2_P to authenticate that the
20 message has been send by the user being the legitimate owner
21 of the pseudonym P.

22 The first embodiment can be implemented in communication
23 networks by neither changing an existing transaction
24 protocol nor changing the structure of a used certificate.
25 Thus, the first embodiment is advantageously applied to
26 environments in which a certificate CERTp issued for a
27 pseudonym P has to comply with an existing certificate
28 format, e.g., in case the format only allows one public key.

1 With reference now to Fig. 3, there is depicted a data
2 exchange according to a second embodiment of the present
3 invention. The second embodiment can advantageously be
4 implemented in an environment in which only the format of
5 the certificate can be changed, e.g., the certificate can
6 include both public keys PK1_P and PK2_P, but no additional
7 data can be added to the request message or the receipt
8 message. Hence, the second public key PK2_P can be directly
9 linked the pseudonym P using only one certificate.

10 Block 300 illustrates a user and block 302 illustrates a PCI
11 as shown in Fig. 2. In response to a user's message
12 requesting a pseudonymous certificate the PCI returns a
13 certificate CERTp. The certificate CERTp securely links
14 both public keys PK1_P and PK2_P to a pseudonym P used by
15 the user. Further it includes information about the issuer,
16 here the PCI, and validation information VAL.

17 With reference now to block 304 illustrating the user
18 previously exchanging data with the PCI and block 306
19 illustrating a transaction server TS communicating with each
20 other. The user creates a transaction request message
21 including the transaction relevant data TRX_P, name of the
22 addressee, here the transaction server TS, and the pseudonym
23 P used by the user, signs the message and sends it to the
24 transaction server TS.

25 After completing the transaction the transaction server TS
26 returns a receipt acknowledging that the requested
27 transaction has been performed. The receipt is a signed
28 message comprising transaction relevant data TRX_T composed
29 by the transaction server TS, the pseudonym P taken from the

1 transaction request message and the name of the issuer of
2 the receipt.

3 Block 308 illustrates the user previously received the
4 receipt and block 310 illustrates a validation server VS1
5 communicating to each other. Whenever the user wants to
6 prove ownership of the receipt the user sends the previously
7 received receipt to the validation server VS1. Furthermore,
8 the user sends a message proving that he is acting
9 legitimately using the pseudonym P.

10 Using the public key PK2_P the validation server
11 authenticates the message presenting the receipt as
12 explained for the scenario of Fig. 2 in greater detail.
13 Alternatively, the user only sends one message as depicted
14 in the data exchange between block 312 illustrating the user
15 owning the receipt and block 314 illustrating an alternative
16 validation server VS2. Here, the user sends a signed message
17 including the receipt previously received from the
18 transaction server TS and two randomizers R1 and R2. Again
19 using the public key PK2_P the validation server
20 authenticates the message presenting the receipt as
21 explained for the scenario shown in Fig. 2.

22 Next, focusing on Fig. 4, there is depicted a data exchange
23 according to a third embodiment of the present invention.
24 The third embodiment can advantageously be implemented in an
25 environment in which only the transaction protocol is
26 allowed to be changed, e.g., in case the certificate CERTp
27 can only include one public key but additional data can be
28 added to the request message and the receipt message
29 respectively.

1 As in Fig. 2 and 3, block 400 of Fig. 4 illustrates a user
2 and block 402 illustrates a PCI. In response to a user's
3 message requesting a pseudonymous certificate the PCI
4 returns a certificate CERTp. In contrast to the embodiment
5 shown in Fig. 3, the certificate CERTp securely links only
6 the first public key PK1_P to a pseudonym P used by the
7 user. Further it includes information about the issuer,
8 here the PCI, and validation information VAL.

9 Block 404 illustrates the user previously exchanging data
10 with the PCI and block 406 illustrates a transaction server
11 TS communicating with each other. The user creates a
12 transaction request message including the transaction
13 relevant data TRX_P, name of the addressee, here the
14 transaction server TS, the pseudonym P used by the user and
15 additionally the second public key PK2_P. Thereafter the
16 user signs the message and sends it to the transaction
17 server TS.

18 The transaction server TS returns a receipt acknowledging
19 that the requested transaction has been performed. The
20 receipt includes transaction relevant data TRX_T composed by
21 the transaction server TS, the pseudonym P taken from the
22 transaction request message, the name of the issuer of the
23 receipt and additionally the second public key PK2_P also
24 taken from the transaction request message. Herewith, the
25 second public key PK2_P is actually linked to the pseudonym
26 P used by the user.

27 Focusing now on block 408 depicting the user having
28 previously received the receipt and block 410 depicting a
29 validation server VS1 communicating to each other. Whenever

1 the user wants to prove ownership of the receipt the user
2 sends the previously received receipt to the validation
3 server VS1. Additionally, the user sends a message proving
4 that he is acting legitimately using the pseudonym P.

5 Using the public key PK2_P obtained together with the
6 receipt the validation server authenticates the message
7 presenting the receipt. Alternatively, the user only sends
8 one message as depicted in the data exchange between block
9 412 illustrating the user owning the receipt and block 414
10 illustrating an alternative validation server VS2. Here,
11 the user sends a signed message including the receipt
12 previously received from the transaction server TS and two
13 randomizers R1 and R2. Again using the public key PK2_P the
14 validation server authenticates the message presenting the
15 receipt as explained for the scenario shown in Fig. 2 and 3.

16 With reference now to Fig. 5, there is depicted a data
17 exchange according to a fourth embodiment of the present
18 invention. The fourth embodiment expects an environment
19 providing complete freedom in the design of the certificate
20 format and transaction protocol. Thus, the transaction
21 protocol as well as the certificate format can be adapted.
22 Furthermore, the fourth embodiment provides anonymity since
23 all pseudonym identifiers have been removed. Therefore, the
24 legitimate user is only identified by a public key. In
25 other words, the user knowing the corresponding private key
26 is the legitimate user of the respective receipt. Hence,
27 the fourth embodiment provides anonymous certificates and
28 transactions. However, in case the PCI only issues
29 anonymous certificates for users providing a certificate

1 CERTu to prove their real identity, it is still possible to
2 track down fraudulent users.

3 Again block 500 illustrates a user and block 502 illustrates
4 a PCI. In response to a user's message requesting a
5 certificate the PCI returns a certificate CERTp. In
6 contrast to the embodiment shown in Fig. 4, the certificate
7 request only includes both public keys and the user's
8 certificate CERTu. Thus, no pseudonym is provided to the
9 PCI. The certificate CERTp securely links both public keys
10 PK1_P and PK2_P together.

11 As in Fig. 4, block 504 illustrates the user previously
12 exchanging data with the PCI and block 506 illustrates a
13 transaction server TS communicating with each other. The
14 user creates a transaction request message including the
15 transaction relevant data TRX_P, the name of the addressee,
16 here the transaction server TS and the second public key
17 PK2_P. In contrast to the previously described embodiments
18 the transaction request message does not contain a pseudonym
19 P. The legitimate user is only referenced by the public key
20 PK2_P. Thereafter the user signs the message and sends it
21 to the transaction server TS.

22 The transaction server TS returns a receipt acknowledging
23 that the requested transaction has been performed. The
24 receipt includes transaction relevant data TRX_T composed by
25 the transaction server TS, the name of the issuer of the
26 receipt and the second public key PK2_P.

27 Block 508 depicts the user having previously received the
28 receipt and block 510 depicting a validation server VS1

1 communicating to each other. Whenever the user wants to
2 prove ownership of the receipt the user sends the previously
3 received receipt to the validation server VS1.
4 Additionally, the user sends a message proving that he is
5 acting legitimately using the pseudonym P. The message
6 includes two randomizers R1 and R2 and the second public key
7 PK2_P.

8 Using the public key PK2_P obtained together with the
9 receipt the validation server authenticates the message
10 presenting the receipt. Alternatively, the user only sends
11 one message as depicted in the data exchange between block
12 512 illustrating the user owning the receipt and block 514
13 illustrating an alternative validation server VS2. In this
14 case, the user sends a signed message including the receipt
15 previously received from the transaction server TS and two
16 randomizers R1 and R2. Again using the public key PK2_P the
17 validation server authenticates the message presenting the
18 receipt.

19 Finally, with reference to Fig. 6, there is depicted a data
20 exchange according to a fifth embodiment of the present
21 invention. As the fourth embodiment, the fifth embodiment
22 expects an environment providing complete freedom in the
23 design of the certificate format and transaction protocol.
24 Like the fourth embodiment, the fifth embodiment also
25 provides anonymity since all pseudonym identifier has been
26 removed. Additionally, the number of key pairs is reduced
27 to one. Hence, only on public key is needed for initiating
28 a transaction and proving ownership of a respective receipt
29 issued in response to the transaction.

1 Therefore, the legitimate user is only identified by one
2 single public key. In other words, the user knowing the
3 corresponding private key is the legitimate user of the
4 respective receipt. Hence, the fifth embodiment provides
5 really anonymous certificates and transactions. However, in
6 the present case the PCI is only necessary if it is desired
7 to be able to track down fraudulent users. Since the only
8 key used, does not need to be linked to a pseudonym or
9 another key the PCI is in fact not necessary for the fifth
10 embodiment.

11 Block 600 illustrates again a user and block 602 illustrates
12 a PCI. In response to a user's message requesting a
13 certificate the PCI returns a certificate CERTp. In
14 contrast to the fourth embodiment shown in Fig. 5, the
15 certificate request only includes one public key PK1_P and
16 the user's certificate CERTu. Thus, no pseudonym is
17 provided to the PCI.

18 As in Fig. 5, block 604 illustrates the user previously
19 exchanging data with the PCI and block 606 illustrates a
20 transaction server TS communicating with each other. The
21 user creates a transaction request message including the
22 transaction relevant data TRX_P, the name of the addressee,
23 here the transaction server TS and the only public key
24 PK1_P. The legitimate user is only referenced by the public
25 key PK1_P. Thereafter the user signs the message and sends
26 it to the transaction server TS.

27 The transaction server TS returns a receipt acknowledging
28 that the requested transaction has been performed. The
29 receipt includes transaction relevant data TRX_T composed by

1 the transaction server TS, the name of the issuer of the
2 receipt and the public key PK1_P.

3 Block 608 depicts the user having previously received the
4 receipt and block 610 depicts a validation server VS1
5 communicating to each other. Whenever the user wants to
6 prove ownership of the receipt the user sends the previously
7 received receipt to the validation server VS1.
8 Additionally, the user sends a message proving that he is
9 acting legitimately using the pseudonym P. The message
10 including two randomizers R1 and R2 and the public key
11 PK1_P.

12 Using the public key PK1_P obtained together with the
13 receipt the validation server authenticates the message
14 presenting the receipt. Alternatively, the user only sends
15 one message as depicted in the data exchange between block
16 612 illustrating the user owning the receipt and block 614
17 illustrating an alternative validation server VS2. In this
18 case, the user send a signed message including the receipt
19 previously received from the transaction server TS and two
20 randomizer R1 and R2. Again using the public key PK1_P the
21 validation server authenticates the message presenting the
22 receipt.

23 The present invention can be realized in hardware, software,
24 or a combination of hardware and software. A visualization
25 tool according to the present invention can be realized in a
26 centralized fashion in one computer system, or in a
27 distributed fashion where different elements are spread
28 across several interconnected computer systems. Any kind of
29 computer system - or other apparatus adapted for carrying

1 out the methods described herein - is suitable. A typical
2 combination of hardware and software could be a general
3 purpose computer system with a computer program that, when
4 being loaded and executed, controls the computer system such
5 that it carries out the methods described herein. The
6 present invention can also be embedded in a computer program
7 product, which comprises all the features enabling the
8 implementation of the methods described herein, and which -
9 when loaded in a computer system - is able to carry out
10 these methods.

11 Computer program means or computer program in the present
12 context include any expression, in any language, code or
13 notation, of a set of instructions intended to cause a
14 system having an information processing capability to
15 perform a particular function either directly or after
16 either or both of the following conversion to another
17 language, code or notation, and/or reproduction in a
18 different material form.

19 Thus the invention includes an article of manufacture
20 comprising a computer usable medium having computer readable
21 program code means embodied therein for causing a function
22 described above. The computer readable program code means
23 in the article of manufacture comprising computer readable
24 program code means for causing a computer to effect the
25 steps of a method of this invention.

26 Similarly, the present invention may be implemented as a
27 computer program product comprising a computer usable medium
28 having computer readable program code means embodied therein
29 for causing a function described above. The computer

1 readable program code means in the computer program product
2 comprising computer readable program code means for causing
3 a computer to effect one or more functions of this
4 invention.

5 Furthermore, the present invention may be implemented as a
6 program storage device readable by machine, tangibly
7 embodying a program of instructions executable by the
8 machine to perform method steps for causing one or more
9 functions of this invention.

10 It is noted that the foregoing has outlined some of the more
11 pertinent objects and embodiments of the present invention.
12 This invention may be used for many applications. Thus,
13 although the description is made for particular arrangements
14 and methods, the intent and concept of the invention is
15 suitable and applicable to other arrangements and
16 applications. It will be clear to those skilled in the art
17 that modifications to the disclosed embodiments can be
18 effected without departing from the spirit and scope of the
19 invention. The described embodiments ought to be construed
20 to be merely illustrative of some of the more prominent
21 features and applications of the invention. Other
22 beneficial results can be realized by applying the disclosed
23 invention in a different manner or modifying the invention
24 in ways known to those familiar with the art.